GCED$^{Q\&As}$

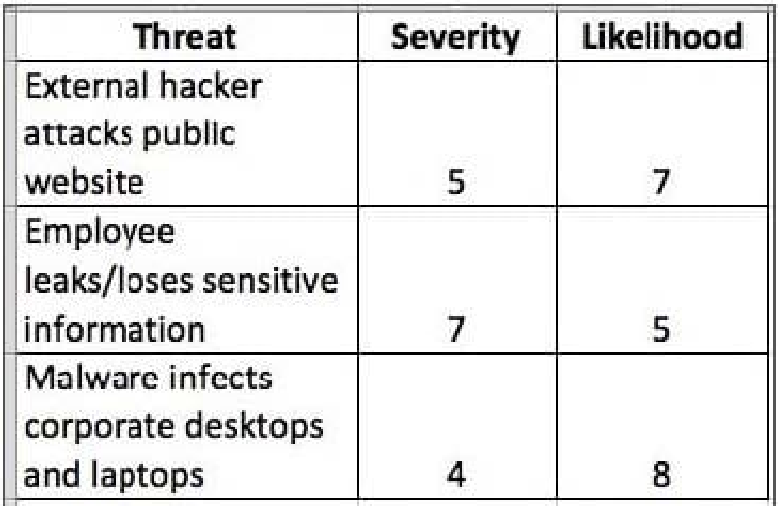
GIAC Certified Enterprise Defender Practice Test

Pass GIAC GCED Exam with 100% Guarantee

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

The matrix in the screen shot below would be created during which process?



Threat	Severity	Likelihood
External hacker attacks public website	5	7
Employee leaks/loses sensitive information	7	5
Malware infects corporate desktops and laptops	4	8

A. Risk Assessment

B. System Hardening

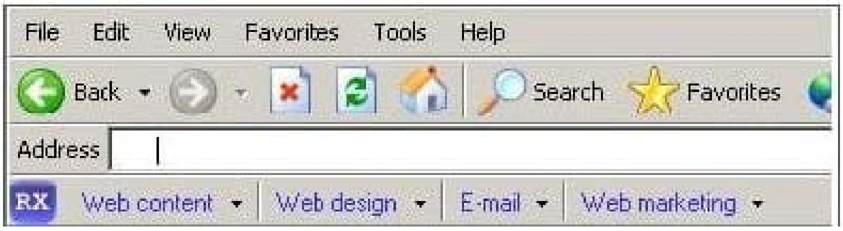
C. Data Classification

D. Vulnerability Scanning

Correct Answer: A

QUESTION 2

Which of the following tools is the most capable for removing the unwanted add-on in the screenshot below?



A. ProcessExplorer

B. Taskkill

C. Paros

D. Hijack This

Correct Answer: B

QUESTION 3

Of the following pieces of digital evidence, which would be collected FIRST from a live system involved in an incident?

A. Event logs from a central repository

B. Directory listing of system files

C. Media in the CDrom drive

D. Swap space and page files

Correct Answer: D

Explanation: Best practices suggest that live response should follow the order of volatility, which means that you want to collect data which is changing the most rapidly. The order of volatility is: Memory Swap or page file Network status and current / recent network connections Running processes Open files

QUESTION 4

How does an Nmap connect scan work?

A. It sends a SYN, waits for a SYN/ACK, then sends a RST.

B. It sends a SYN, waits for a ACK, then sends a RST.

C. It sends a SYN, waits for a ACK, then sends a SYN/ACK.

D. It sends a SYN, waits for a SYN/ACK, then sends a ACK

Correct Answer: A

Explanation: An Nmap connect scan sends a SYN, waits for a SYN/ACK, then sends a ACK to complete the three-way handshake. A Nmap half-open scan sends a SYN, waits for a SYN/ACK, then sends a RST.

QUESTION 5

A security device processes the first packet from 10.62.34.12 destined to 10.23.10.7 and recognizes a malicious anomaly. The first packet makes it to 10.23.10.7 before the security devices sends a TCP RST to 10.62.34.12. What type of security device is this?

A. Host IDS

B. Active response

C. Intrusion prevention

D. Network access control

Correct Answer: B

An active response device dynamically reconfigures or alters network or system access controls, session streams, or individual packets based on triggers from packet inspection and other detection devices. Active response happens after the event has occurred, thus a single packet attack will be successful on the first attempt and blocked in future attempts. Network intrusion prevention devices are typically inline devices on the network that inspect packets and make decisions before forwarding them on to the destination. This type of device has the capability to defend against single packet attacks on the first attempt by blocking or modifying the attack inline.